UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,242	06/26/2001	Zheng Qi	1875.9090002	3440

26111 7590 04/25/2007

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PICH, PONNOREAY	
ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/892,242	QI ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-8,13-19,21,23,26-34,36,38 and 41-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-8,13-19,23,27-34,38,42 and 43* is/are rejected.

7)☒ Claim(s) *4,21,26,36,41* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to supplemental amendments filed on 11/22/2006. The indications of allowable claims from the prior office action are withdrawn due to newly discovered prior art (Kawamura et al: US 6,940,975). Any inconvenience is regretted. Claims 1, 4-8, 13-19, 21, 23, 26-34, 36, 38, and 41-43 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 14-19, 23, 30-34, and 42 are rejected under 35 U.S.C. 102(e) as being anticipated by Kawamura et al (US 6,940,975).

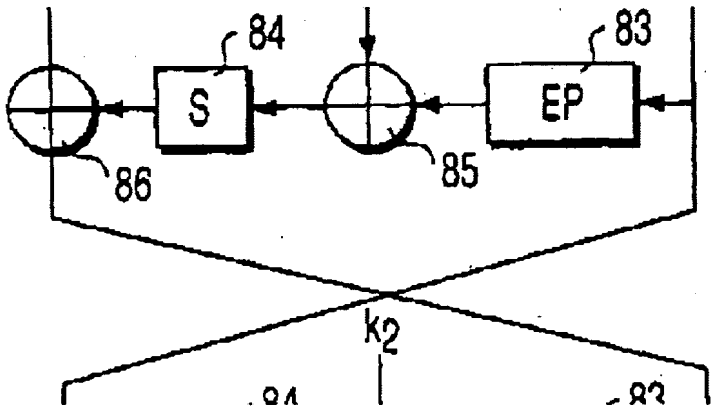
Claims 1 and 23:

Kawamura discloses:

1. A key scheduler (Fig 1, item 2 and Fig 16-18) configured to provide keys for cryptographic operations (Fig 13, k1, k2...k16).
2. Expansion logic (Fig 13, item 83 or Fig 13, items 81a and 83) configured to expand a first bit sequence having a first size to an expanded first bit sequence having second size greater than the first size, the first sequence corresponding to

a right portion of an input bit sequence for the current cryptographic round (col 11, lines 45-53).

3. First circuitry configured to perform an exclusive OR (XOR) on the expanded first bit sequence and a key provided by the key scheduler to generate a third bit sequence (Fig 13, item 85).
4. A substitution box (Sbox) configured to transform the third bit sequence into a fourth bit sequence (Fig 13, item 84).
5. Second circuitry configured to perform an exclusive OR (XOR) on the fourth bit sequence and a left portion of the input bit sequence for the current cryptographic round to generate a fifth bit sequence (Fig 13, item 86).
6. Permutation logic coupled to the expansion logic and the second circuitry, the permutation logic configured to receive the fifth bit sequence from the second circuitry and to perform a permutation on the fifth bit sequence (Fig 13, item 83 of next round).
7. Wherein the fifth bit sequence is a right portion of an output bit sequence of a current cryptographic round (Fig 13).



Note that the above portion from Figure 13 shows one round of the cryptographic engine. The output from item 86, i.e. the fifth bit sequence, is the right portion of an output bit sequence of a cryptographic round.

Claim 14:

Kawamura further discloses wherein the key scheduler comprises a plurality of stages (Fig 16, stage 111, 112, and 113 and Fig 18).

Claims 15-18 and 30-33:

Kawamura further discloses wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage, and a consumption stage (col 14, lines 5-15; Figures 16-18; and Fig 1, items 2 and 8).

Claims 19 and 34:

Kawamura further discloses wherein a first shift amount for a first key is identified in a determination stage using a first round counter value (col 13, line 10-col 14, line 60).

Claim 42:

Kawamura further discloses:

1. A first expansion logic block coupled to the first circuitry and configured to receive the first bit sequence (Fig 13, item 83 of first round).
2. A second expansion logic block coupled to the second circuitry and to the first circuitry configured to receive the fifth bit sequence from the second circuitry (Fig 13, item 83 of second round).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5-8 and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura et al (US 6,940,975) in view of Ritter (US 5,727,062).

Claim 5:

Kawamura does not explicitly disclose wherein the first bit sequence is less than 32 bits. However, Ritter discloses variable sized block cryptography which can be incorporated within DES (col 7, lines 47-50 and col 9, lines 19-21). Ritter disclose that the layers of his invention operate on small units of data, i.e. one byte wide (col 9, lines 28-30 and col 11, lines 40-52). In light of Ritter's teachings, it would have been obvious to one of ordinary skill in the art to modify Kawamura's invention such that the input bit

sequence was variable in size and such that the first bit sequence was less than 32 bits. One skilled would have been motivated to do so because use of simple operations which operates on small units are easy to extend to any size and offers higher speed ciphers (Ritter: col 9, lines 40-52).

Claims 6 and 27:

Kawamura does not explicitly disclose the first bit sequence is four bits. However, Ritter's cryptography teachings allow for variable block sizes such that small units of data are operated upon (col 7, lines 47-50; col 9, lines 19-30; and col 11, lines 40-52). Ritter does not place any limit on how small a block size can be worked upon by his invention, thus it would have been obvious to modify Kawamura's invention in light of Ritter's teachings so that the first bit sequence is four bits. One skilled would have been motivated to do so because Ritter discloses operations on small units are easy to extend to any size and offer high speed ciphers (col 9, lines 40-52).

Claim 7:

Kawamura and Ritter disclose all the limitations of claims 5 and 23. Ritter further discloses that the expanded first bit sequence is less that 48 bits (col 9, lines 28-30 and col 11, lines 40-52).

Claims 8 and 28:

Kawamura and Ritter disclose all the limitations of claims 6 and 27. Ritter further discloses wherein the expanded first bit sequence is less than six bits (col 7, lines 47-50; col 9, lines 19-30; and col 11, lines 40-52). Ritter does not place any limitations on how small the units of data operated upon can be, thus the data can be less than six

bits. One skilled would have been motivated to make it small, i.e. less than six bits, because small units are easy to extend to any size and offer high speed ciphers (col 9, lines 40-52).

Claims 13 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura et al (US 6,940,975) in view of Windirsch (US 6,769,063).

Claims 13 and 29:

Kawamura does not explicitly disclose the key scheduler performs pipelined key scheduling logic. However, Windirsch teaches pipeline being used in an encryption/decryption device (col 2, lines 12-35). At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Kawamura's key scheduler such that it performed pipelined key scheduling. One of ordinary skill would have been motivated to do so because it would allow for simultaneous processing of a number of data streams as disclosed by Windirsch (col 2, lines 12-16).

Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura et al (US 6,940,975).

Claim 38:

Kawamura discloses an XOR operation for combining the key provided by the key scheduler with the expanded first bit sequence (Fig 13, item 85).

Kawamura does not explicitly disclose the XOR operation being simulated by a plurality of logic device, the plurality of logic devices including a multiplexer receiving a first and second input values and an OR logic combining an output value of the multiplexer with a third input value; wherein the first, second, and third values a determined based on the key provided by the key scheduler and further based on a select value indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations. However, official notice is taken that it was well known to one of ordinary skill in the art at the time applicant's invention was made that an XOR operation could be simulated via use of a multiplexer, an OR gate/logic, and one or more control signals. It would have been obvious to one of ordinary skill in the art to modify Kawamura's invention according to the limitations recited in claim 38 by substituting the XOR logic seen in Figure 13 with a plurality of logic devices recited in claim 38. One of ordinary skill would have been motivated to do so because use of certain equivalent logic circuits are often used in place of another to achieve desired circuit timing.

Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura et al (US 6,940,975) in view of Sutherland (US 4,679,213).

Claim 43:

Kawamura does not explicitly disclose a first asynchronous FIFO configured to convert input blocks of a third size to blocks of a fourth size for cryptographic processing; and a second asynchronous FIFO configured to convert cryptographic output blocks of the fourth size to the third size for further processing.

However, Sutherland discloses that asynchronous FIFO's were well known in the art at the time applicant's invention was made (col 1, lines 26-44 and 5-24). At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to implement an asynchronous input FIFO and an asynchronous output FIFO within Kawamura's system according to the limitations recited in claim 43 so that input and output data are buffered. One skilled would have been motivated to do so because it would allow time independence between a user inputting data to be encrypted and the data being processed as well as between the time the data is processed from the time it is read. Note that because the data are buffered at the input and the output via use of asynchronous input and output FIFO's, data that are of a third size are converted to a fourth size at the first/input FIFO and from a fourth size to a third size and the output/second FIFO.

Allowable Subject Matter

Claims 4, 21, 41, 26, and 36 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The claims are allowable for the limitation further recited in claims 4 and 26. Claims 21 and 41 are dependent on claim 4 and claim 36 is depended on claim 26.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100